REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Chi fa cosa? L'autenticazione e l'autorizzazione nelle infrastrutture di sicurezza complessa

Gabriella Cattaneo

Security Technical Engineer

Sun Microsystems, Inc.

Chi fa cosa?

- Come distinguere i buoni dai cattivi?
- Come identificare le persone?
- Come verificare l'identità delle persone?
- Come garantire i giusti diritti di accesso?
- Come evitare le fughe di informazioni?

Chi fa cosa?

- Identificazione
  - Chi sono?
- Autenticazione
  - Ti dimostro che sono proprio io!
- Autorizzazione
  - Dove posso andare?

Identificazione

- Chi sono le persone che accedono alle informazioni?

- Classificazione degli utenti
  - Identificazione personale
  - Identificazione di gruppo
- Richiesta di autenticazione

Autenticazione

- Qualcosa che uno sa
  - Un utente è identificato dalla conoscenza di una informazione segreta: una password, una chiave crittografica segreta, un PIN...
- Qualcosa che uno ha
  - Un utente è identificata tramite il possesso di uno oggetto fisico: smart card, token card...
- Qualcosa che uno è
  - Un utente è identificato da un suo tratto fisico peculiare: le impronte digitale, l'immagine dell'iride...

Autenticazione statica: password

- Veloce da realizzare, economica e realizzata via software.
- Criticità:
  - Segretezza della password
  - Invio della password
  - La conservazione della password sul sistema
  - La password di nuove utenze
  - L'aggiornamento della password

La scelta della password

Autenticazione robusta

- One-time password
- Token card
- Certificati e firma digitale
- Smart card

- Autenticazione continua

Autenticazione Biometrica

- L'impronta digitale
  - Metodo più diffuso e meno costoso.
- La retina
- L'iride.
  - Metodo più efficiente ma più costoso
- Caratteristica tridimensionale della mano e/o del viso.
- La firma calligrafica.

Autorizzazione

Autorizzazione

- Associa ad ogni utente le operazioni permesse e proibite
- "Tutti gli accessi sono proibiti, se non espressamente permessi"
  - Need-to-know
- "Tutti gli accessi sono permessi, se non espressamente proibiti"

Come mettere insieme i vari pezzi?

Gestione centralizzata dell'Identità

I requisiti fondamentali

1. Indipendente dalla Piattaforma e approccio basato sugli standard
2. Un'architettura robusta e sicura che aiuta a soddisfare i requisiti di legge e a ridurre i rischi
3. Una federazione dei servizi che scambiano informazioni affidabili e sicure sull'identità

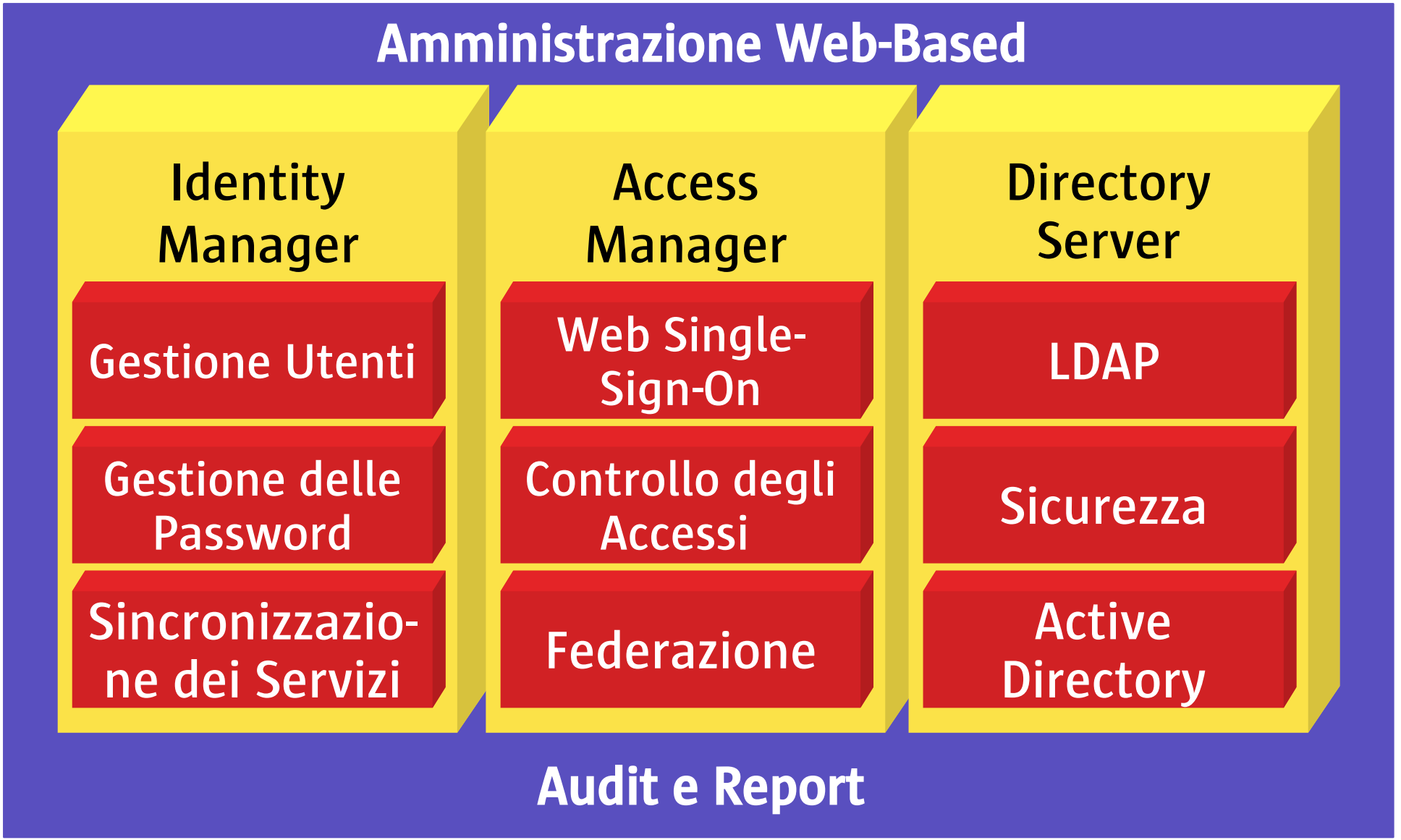
Gli elementi della soluzione

Directory Server

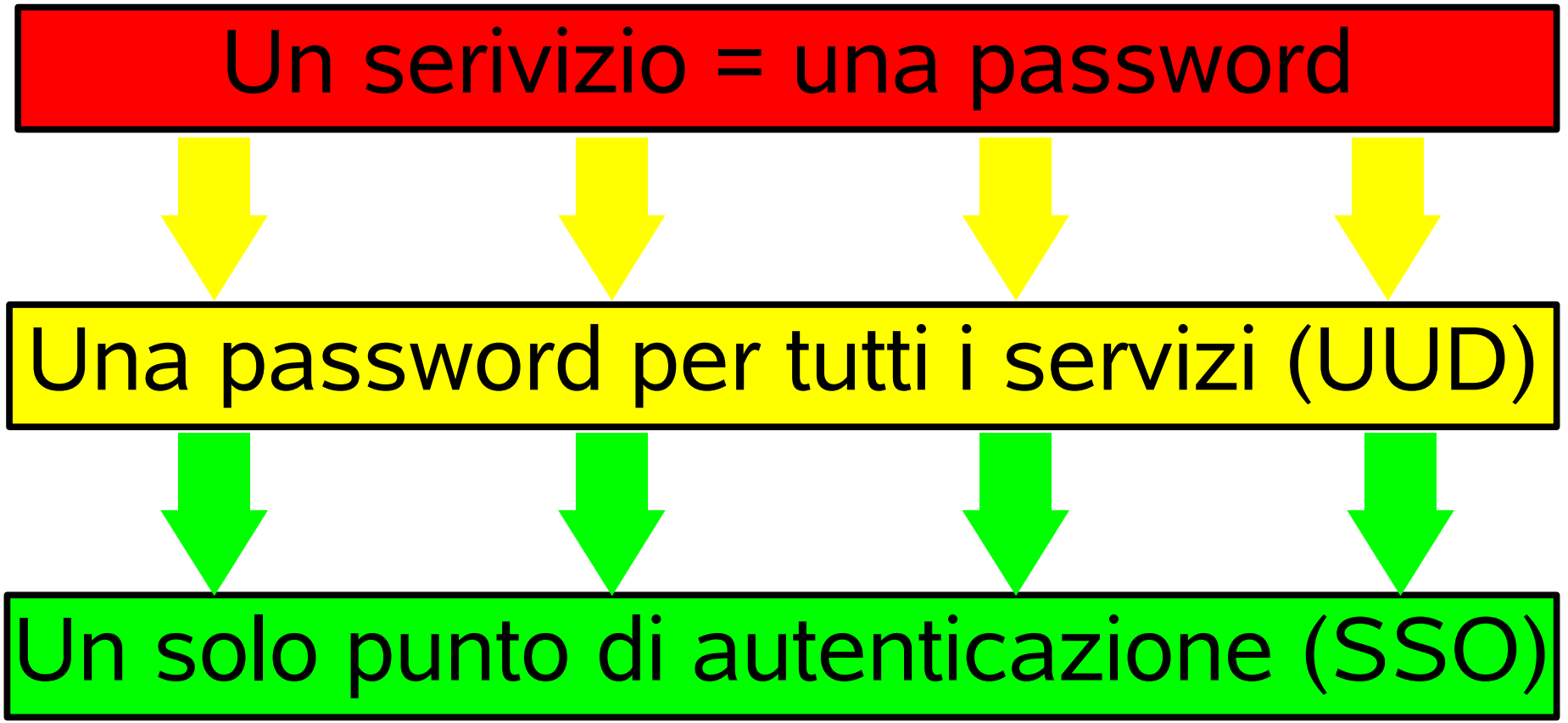
Identity Manager

Access Manager

Gli elementi della soluzione



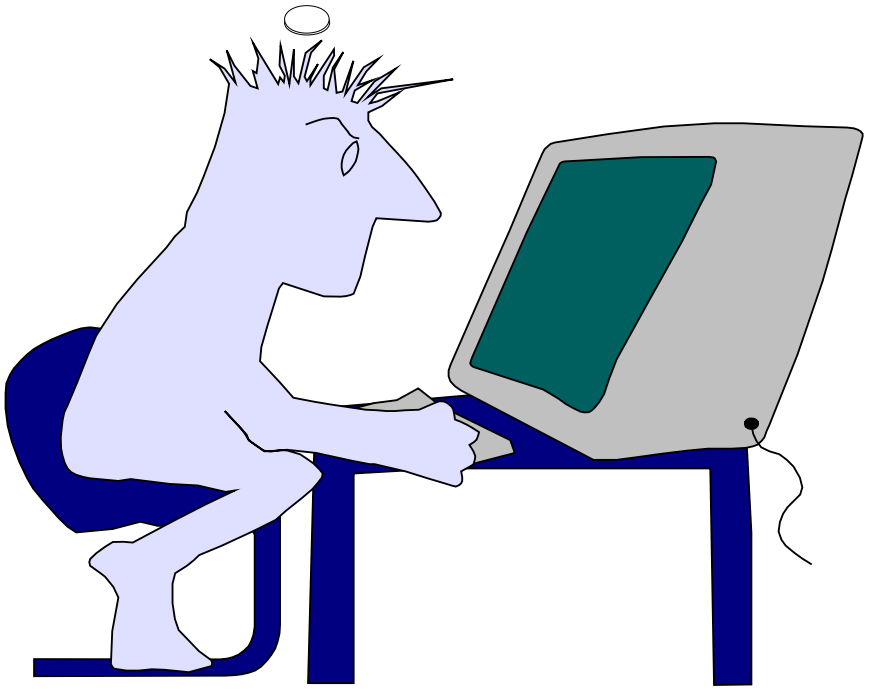
Single Sigh On



Siamo sicuri del servizi richiesti?

Mi posso fidare a dare il numero della carta di credito?

Chi sa se sono sul server giusto?



REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Gabriella Cattaneo

Security Technical Engineer

Sun Microsystems, Inc.